PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-003256

(43)Date of publication of application : 06.01.1998

(51)Int.Cl. G09C 1/00

G09C 1/00

G09C 1/00

G11B 20/10

H04L 9/08

H04L 9/06

H04L 9/14

(21)Application number : 08-269502 (71)Applicant : SONY CORP

(22)Date of filing : 11.10.1996 (72)Inventor : ISHIGURO RYUJI

(30)Priority

Priority number :	07267249	Priority date : 16.10.1995	Priority country : JP
	07267250	16.10.1995	JP
	08 93800	16.04.1996	JP

(54) CIPHERING METHOD AND DEVICE THEREFOR, RECORDING METHOD, DECODING METHOD AND DEVICE THEREFOR AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To easily control the ciphering key.

SOLUTION: A ciphering key K1 is generated from a master key K0 using a unidirectional function, a next ciphering key K2 is generated from the key K1 using the function and similarly n-hierarchial ciphering keys K1 to Kn are generated. Then, information is ciphered by the key Kn and the information is decoded by the ciphering key Kn. If the key Kn is read, the information is ciphered by the key Kn-1 and the information is decoded by the key Kn-1. Thus, the information, which is ciphered by the key Kn, is decoded by the key Kn obtained from the key Kn-1 using the function and the user is only required to maintain the latest key Kn-1.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's

decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The encryption approach which hierarchizes the above-mentioned cryptographic key using a one-way function, and is characterized by enciphering the above-mentioned predetermined information using the cryptographic key by which hierarchization was carried out [above-mentioned] in the encryption approach which enciphers predetermined information using a predetermined cryptographic key.

[Claim 2] The cryptographic key of the beginning when hierarchizing among the hierarchized above-mentioned cryptographic keys is the encryption approach according to claim 1 characterized by being a master key.

[Claim 3] The encryption approach according to claim 1 characterized by enciphering specific information using the cryptographic key by which hierarchization was carried out [above-mentioned].

[Claim 4] The record approach characterized by receiving the predetermined information enciphered in the record approach which records the enciphered predetermined information on a record medium using the cryptographic key hierarchized using the one-way function, and recording the predetermined information by which encryption was carried out [above-mentioned] on the above-mentioned record medium.

[Claim 5] The record approach according to claim 4 characterized by recording the specific information by which received the specific information enciphered

using the above-mentioned cryptographic key, and encryption was carried out [above-mentioned] with the predetermined information by which encryption was carried out [above-mentioned] on the above-mentioned record medium.

[Claim 6] The decryption approach characterized by decrypting the predetermined information enciphered using the decryption key corresponding to the cryptographic key which received the enciphered predetermined information in the decryption approach which decrypts the enciphered predetermined information, and was hierarchized using the one-way function.

[Claim 7] The cryptographic key of the beginning when hierarchizing among the hierarchized above-mentioned cryptographic keys is the decryption approach according to claim 6 which is a master key and is characterized by generating the decryption key corresponding to a cryptographic key from the above-mentioned master key using a one-way function.

[Claim 8] The decryption approach according to claim 6 characterized by decrypting the predetermined information by which determined the above-mentioned decryption key from the information for receiving the enciphered specific information and determining the above-mentioned specific information which is not enciphered, the enciphered above-mentioned specific information, and the above-mentioned decryption key, and encryption was carried out [above-mentioned] using the determined decryption key.

[Claim 9] The above-mentioned information for determining the above-mentioned decryption key is a master key or the decryption approach according to claim 8 characterized by being the information on the newest cryptographic key.

[Claim 10] The above-mentioned decryption key is the decryption approach according to claim 8 which carries out the description of what is determined by the step which compares the step which decrypts the specific information by which encryption was carried out [above-mentioned] with the above-mentioned specific information which is not enciphered as the decrypted specific information using the above-mentioned information for determining the above-mentioned decryption key, and determines the above-mentioned decryption key based on a

comparison result.

[Claim 11] When the above-mentioned specific information which is not enciphered as the decrypted above-mentioned specific information is not in agreement, It asks for the new above-mentioned decryption key hierarchized using the up Norikazu directional function from the information for determining the above-mentioned decryption key. The actuation which decrypts the above-mentioned specific information enciphered using the new decryption key When the above-mentioned specific information which is not enciphered as the decrypted above-mentioned specific information is in agreement repeatedly until the above-mentioned specific information which is not enciphered as the decrypted above-mentioned specific information was in agreement, The decryption approach according to claim 10 characterized by using the above-mentioned decryption key at that time as the final above-mentioned decryption key.

[Claim 12] It is the decryption approach according to claim 6 which the predetermined information by which encryption was carried out [above-mentioned] is recorded on the record medium, and the information on predetermined [which was enciphered] is supplied by carrying out reading appearance from the above-mentioned record medium, and carries out the description of the above-mentioned cryptographic key being printed as the alphabetic character corresponding to the above-mentioned cryptographic key, a figure, a bar code, or a hologram on the case which contains the above-mentioned record medium or the above-mentioned record medium.

[Claim 13] The above-mentioned cryptographic key is the decryption approach according to claim 6 characterized by being inserted as a code corresponding to the above-mentioned cryptographic key into the predetermined software for decrypting the enciphered predetermined information.

[Claim 14] The above-mentioned cryptographic key is the decryption approach according to claim 6 which carries out the description of being supplied through the telephone line or a network.

[Claim 15] Encryption equipment characterized by having a generating means to generate the above-mentioned cryptographic key by hierarchizing predetermined information in the encryption equipment enciphered using a predetermined cryptographic key using a one-way function, and an encryption means to encipher the above-mentioned predetermined information using the cryptographic key by which hierarchization was carried out [above-mentioned].
[Claim 16] The cryptographic key of the beginning when hierarchizing among the hierarchized above-mentioned cryptographic keys is encryption equipment according to claim 15 characterized by being a master key.
[Claim 17] Encryption equipment according to claim 15 characterized by having further the 2nd encryption means which enciphers specific information using the cryptographic key by which hierarchization was carried out [above-mentioned].
[Claim 18] Decryption equipment characterized by having a decryption means to decrypt the predetermined information enciphered as a receiving means to receive the enciphered predetermined information in the decryption equipment which decrypts the enciphered predetermined information, using the decryption key corresponding to the cryptographic key hierarchized using the one-way function.
[Claim 19] The 1st storage means which memorizes the information for determining the decryption key corresponding to the above-mentioned cryptographic key, A generation means to generate the decryption key corresponding to the above-mentioned cryptographic key from a master key using a one-way function, The information for having further the 2nd storage means which memorizes the decryption key corresponding to the cryptographic key by which generation was carried out [above-mentioned], and determining the decryption key corresponding to the cryptographic key Decryption equipment according to claim 18 characterized by being the master key which is the cryptographic key of the beginning when hierarchizing among the hierarchized above-mentioned cryptographic keys.
[Claim 20] The above-mentioned receiving means receives the enciphered

specific information. The above-mentioned generation means From the information for determining the decryption key corresponding to the above-mentioned specific information which is not enciphered, the specific information enciphered, and the above-mentioned cryptographic key It is decryption equipment according to claim 19 which determines the decryption key corresponding to the cryptographic key which enciphered the received above-mentioned predetermined information, and is characterized by the above-mentioned decryption means decrypting the predetermined information by which encryption was carried out [above-mentioned] using the determined decryption key.

[Claim 21] The above-mentioned information for determining the decryption key corresponding to the above-mentioned cryptographic key is a master key or decryption equipment according to claim 20 characterized by being the information on the newest cryptographic key.

[Claim 22] The above-mentioned generation means is decryption equipment according to claim 21 which carries out the description of decrypting the specific information by which encryption was carried out [above-mentioned] using the above-mentioned information for determining the decryption key corresponding to the above-mentioned cryptographic key, comparing the specific information and above-mentioned specific information which were decrypted, and determining the decryption key corresponding to a cryptographic key based on a comparison result.

[Claim 23] When the above-mentioned specific information of the above-mentioned generation means which is not enciphered as the decrypted above-mentioned specific information does not correspond, It asks for the new above-mentioned decryption key hierarchized using the up Norikazu directional function from the information for determining the above-mentioned decryption key. The actuation which decrypts the above-mentioned specific information enciphered using the new decryption key When the above-mentioned specific information which is not enciphered as the decrypted above-mentioned specific information is

in agreement repeatedly until the above-mentioned specific information which is not enciphered as the decrypted above-mentioned specific information was in agreement, Decryption equipment according to claim 22 characterized by making the storage means of the above 2nd memorize the above-mentioned decryption key at that time.

[Claim 24] The storage means of the above 1st, the storage means of the above 2nd, the above-mentioned generation means, and the above-mentioned decryption means are decryption equipment according to claim 19 characterized by being arranged in one IC chip.

[Claim 25] The information for determining the decryption key corresponding to the above-mentioned cryptographic key is decryption equipment according to claim 24 characterized by what is beforehand memorized by the 1st storage means.

[Claim 26] It is the record medium which has the record signal which can be decoded with decryption equipment in the record medium which can be decoded with decryption equipment, and carries out the description of the above-mentioned record signal including the predetermined information enciphered using the cryptographic key hierarchized using the one-way function.

[Claim 27] The above-mentioned record signal is a record medium according to claim 26 characterized by including further the specific information enciphered using the above-mentioned cryptographic key.

[Claim 28] The above-mentioned cryptographic key is a record medium according to claim 26 which carries out the description of being printed by the above-mentioned record medium as the alphabetic character corresponding to the above-mentioned cryptographic key, a figure, a bar code, or a hologram.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention uses, when preventing the unauthorized use of the software, the data, etc. supplied through the software recorded on record media, such as a digital video disc (DVD), by the encryption approach, encryption equipment, the record approach, the decryption approach, decryption equipment, and the record approach, concerning the record medium with which information was recorded, data, or a network, and it relates to the suitable encryption approach, encryption equipment, the record approach, the decryption approach, decryption equipment, and a record medium.

[0002]

[Description of the Prior Art] Usually, when preventing the unauthorized use of software or data, it enciphers using a predetermined cryptographic key, and he records this enciphered software or data on a digital video disc (it is hereafter described as DVD), or is trying to supply software and data through a network. And the enciphered software or data which was offered through DVD or the network is decrypted using the above-mentioned cryptographic key supplied separately.

[0003] Here, informational encryption and an informational decryption are explained briefly. Drawing 12 shows the principle about informational encryption and an informational decryption. Plaintext M (information to transmit) is enciphered with the encryption block 101 at a delivery side using the encryption key K1, and Cipher C (data transmitted actually) is generated. The cipher C is transmitted to a receptacle side, it is decrypted with the decryption block 102 at a receptacle side using the decryption key K2, and Plaintext M is generated. Thus, a plaintext is sent to a receptacle side from a delivery side.

[0004] Moreover, those (decode person) who do not have a decryption key may intercept Cipher C, and may decode the cipher C with the decode block 103. In addition, it is called "decode" that those who do not have "decode", a call, and a decryption key for those who have a decryption key generating Plaintext M from

Cipher C using a decryption key intercept Cipher C, and gain a plaintext from Cipher C here.

[0005] By the way, when enciphering using a cryptographic key which was mentioned above, once it will cryptographic key decode, this cryptographic key will become an invalid to prevention of an unauthorized use henceforth. So, when a cryptographic key is decoded, it is possible by updating a cryptographic key to another thing and performing software or a data encryption using a new cryptographic key to prevent the unauthorized use.

[0006]

[Problem(s) to be Solved by the Invention] However, since the software or data enciphered by the former cryptographic key may exist actually even if it updates a cryptographic key, a former cryptographic key must also be held for the decryption. For this reason, the cryptographic key which should be held whenever a cryptographic key is updated increased, and the technical problem for which management of a cryptographic key becomes less easy also in hardware and by software occurred.

[0007] Moreover, when the cryptographic key is beforehand incorporated in hardware, it may be very difficult to update it to a new cryptographic key itself.

[0008] This invention is made in view of such a situation, and the object of this invention hierarchizes a cryptographic key and is to offer the encryption approach which makes management of a cryptographic key easy, encryption equipment, the record approach, the decryption approach, decryption equipment, and a record medium.

[0009]

[Means for Solving the Problem] The encryption approach according to claim 1 is characterized by hierarchizing a cryptographic key using a one-way function, and enciphering predetermined information using the hierarchized cryptographic key.

[0010] The record approach according to claim 4 is characterized by receiving the predetermined information enciphered using the cryptographic key hierarchized using the one-way function, and recording the enciphered

predetermined information on a record medium.

[0011] The decryption approach according to claim 6 receives the enciphered predetermined information, and is characterized by decrypting the predetermined information enciphered using the decryption key corresponding to the cryptographic key hierarchized using the one-way function.

[0012] Encryption equipment according to claim 15 is characterized by having a generating means to generate a cryptographic key, and an encryption means to encipher predetermined information using the hierarchized cryptographic key by hierarchizing using a one-way function.

[0013] Decryption equipment according to claim 18 is characterized by having a decryption means to decrypt the predetermined information enciphered as a receiving means to receive the enciphered predetermined information, using the decryption key corresponding to the cryptographic key hierarchized using the one-way function.

[0014] A record medium according to claim 26 has the record signal which can be decoded with decryption equipment, and a record signal carries out the description of including the predetermined information enciphered using the cryptographic key hierarchized using the one-way function.

[0015] the above -- in the case of which, what was hierarchized by the one-way function as a cryptographic key is used.

[0016]

[Embodiment of the Invention] Drawing 1 is drawing showing the example of the approach of hierarchization of the cryptographic key which applied the encryption approach of this invention. In this drawing, the next hierarchy's (Ver.n) cryptographic key K1 is formed to the first hierarchy's cryptographic key (master key (Masterkey) (K0)) using the so-called one-way function F (one-way Function). Here, it is F. It is one [so-called] of the one-way functions, and although it can perform easily calculating K1 from a cryptographic key K0, the operation of the reverse, i.e., calculate K0 from a cryptographic key K1, is the function which performs an irreversible operation which is very difficult.

[0017] In a one-way function, Data Encryption Standard (DES, National Bureau of Standards FIPS Publication 46, 1977), Fast Encryption Algorithm (FEAL, S.Miyaguchi.The FEAL cipher family.Lecture Notes in Computer Science, and 537 (1001) --) Encryption algorithm like pp627-638. (Advances in Cryptology-CRYPTO'90), Or Message Digest algorithm MD4, R.L.Rivest.The MD4 message digest algorithm.Lecture Notes in Computer Science, and 537 (1001) -- 303-311. () [Advances] in Cryptology-CRYPTO '90 and SecureHash Standard A message digest algorithm as shown in (SHS, Secure Hash Standard.National Bureau of Standards FIPS Publication 180, and 1993) can be used. In addition, DES and FEAL are indicated by the detail in "Tsujii, Kasahara, and "code and information security" and July, 1993." Then, an example is given and a one-way function is explained briefly.

[0018] In the case of DES, relation between a one-way function and DES as shown in a degree type (1) is. Namely, [0019]

F(k)=DES(IV,k)

(Here, iV is initiai Vector and arbitration and k are a key)

... (1)

It comes out.

[0020] Moreover, as an algorithm used for a one-way function, there is the following, for example.

[0021] - block Algorithm of a cipher (product cipher) system.

- Number theory-algorithm.

[0022] block As shown in a degree type (2), the algorithm of a cipher (product cipher) system enciphers a plaintext (Plain text) using a key (key), and acquires a cipher (Cipher text).

[0023]

C=Enc(P,k)

(However, C cipher text and P plain text and k key (key))

... (2)

[0024] Namely, it is hash of a certain kind for every block to key. By function,

conversion which cannot return is performed and a fixed-length bit string is obtained.

[0025] Next, plain permutation which performs text for replacement of data etc. box and substitution It is number round **** to box. At each round, the bit string obtained from key and an operation (Exor) of a certain kind, for example, EXCLUSIVE OR operation, are performed.

[0026] moreover, a number theory-algorithm is shown in a degree type (3) -- as -- dispersion -- a logarithm -- it is used for a problem.

[0027]

F(k) <==> ak mod p (however, a a predetermined constant and k a key and p prime factor)

... (3)

[0028] In addition, in the above-mentioned formula (3), the notation "<==>" means "the definition."

[0029] That is, function F (k) is defined as "just because it broke by p what squared a k." In this case, although it can ask for F (k) easily from a key (k), it is dramatically difficult to ask for F (k) to k.

[0030] thus, after a cryptographic key K1 is called for from the master key K0 using a one-way function (F), it is similarly shown in a degree type (4) using a one-way function (F) -- as -- one by one -- cryptographic keys K2 and K3 and ... Kn-1 and Kn calculate and the cryptographic key hierarchized (Ver.n thru/or Ver.1) is formed.

[0031]

Ki=F (Ki-1) (however, i= 1, 2 and 3, ..., n) ... (4)

[0032] In addition, a numeric value n is the number of hierarchies (generation number) considered to be enough. Therefore, although it can perform easily newly calculating a cryptographic key using a one-way function (F) as mentioned above, it is very difficult to calculate the original key from the cryptographic key calculated using the operation of the reverse, i.e., a one-way function.

[0033] The approach of enciphering the information on the software in this

invention or data, and providing a user here is explained. When enciphering the information on software or data and providing for a user, it attaches to the information which the cryptographic key Kn (Ver.1) was used [information] first, and information was enciphered [information], and had the cryptographic key Kn enciphered, or it supplies separately, and is made to supply a user widely, as shown in drawing 1 . A user can decrypt the enciphered information using a cryptographic key Kn.

[0034] And when this cryptographic key Kn is decoded, the information on software or data is enciphered using cryptographic key Kn-1 of the hierarchy on one (Ver.2), and cryptographic key Kn-1 is distributed to a user. Information is enciphered using the cryptographic key of the hierarchy on one of the cryptographic keys decoded like the following whenever the cryptographic key was decoded, and the cryptographic key is distributed to a user.

[0035] For example, the lowest hierarchy's (Ver.1) cryptographic key Kn distributed first is calculated using Function F from cryptographic key Kn-1 of the next hierarchy (Ver.2). That is, by using Function F, a cryptographic key Kn can be easily calculated from cryptographic key Kn-1, and the information enciphered by the cryptographic key Kn can be decrypted using the cryptographic key Kn calculated from cryptographic key Kn-1. Hereafter, in every generation, the following cryptographic key can be similarly calculated by using Function F.

[0036] Therefore, the user only holds the newest cryptographic key which is not decoded, and can decrypt not only the information enciphered by the newest cryptographic key but the information enciphered by the former cryptographic key. Moreover, all cryptographic keys are keys by which sequential generation is carried out from a master key using the tropism function F on the other hand. Therefore, the user only holds the master key instead of the newest cryptographic key which is not decoded, and can decrypt the information enciphered by all cryptographic keys. Thereby, management of a cryptographic key can be made easy.

[0037] Drawing 2 is a flow chart for explaining the procedure when enciphering

and recording information (plaintext data-lain text), such as an animation, voice, data, and software, on record media, such as a disk (for example, DVD), using the cryptographic key shown in the side which creates a disk at drawing 1 . First, in step S1, a suitable generation's (hierarchy) cryptographic key is chosen among the hierarchized cryptographic keys which were shown in drawing 1 , and the selected cryptographic key is chosen as a work-piece key (work key). Next, it progresses to step S2, the train of the predetermined figure decided beforehand or an alphabetic character is made into a magic number (magic number), and it enciphers using the work-piece key which chose the magic number at step S1. And the enciphered magic number (encrypted magic number) which was obtained by encryption is recorded on the predetermined location of DVD1, as shown in drawing 3 .

[0038] Next, in step S3, information, i.e., plaintext data, to hide is enciphered using a work-piece key, and the enciphered information (cipher text) is recorded on the predetermined location of DVD1.

[0039] Next, the encryption equipment corresponding to the encryption approach mentioned above is explained using drawing 4 . Plaintext data and a magic number are supplied to the encryption circuits 51 or 52 which correspond through each input terminal. The work-piece key generation circuit 53 chooses a suitable generation's (hierarchy) cryptographic key among the hierarchized cryptographic keys which were shown in drawing 1 , and supplies it to the encryption circuits 51 and 52 by using the selected cryptographic key as a work-piece key. The encryption circuit 52 is enciphered using the work-piece key to which the supplied magic number was supplied from the work-piece key generation circuit 53. And the enciphered magic number is supplied to a recording device 54.

[0040] Moreover, the encryption circuit 51 enciphers the supplied plaintext data using a work-piece key, and supplies the enciphered information to a recording device 54. And a recording apparatus 54 records the information and the enciphered Magic information by which the code was carried out on the predetermined location of DVD1, as shown in drawing 3 . In addition, when this

recording apparatus 54 is the formatter which generates a master disc, La Stampa is formed from that original recording, and the disk of a large quantity is produced after that using that La Stampa.

[0041] Drawing 5 is the block diagram showing the example of a configuration of IC chip which decrypts enciphered information which was recorded on DVD1 in the disk player (DVD player) which reproduces DVD1 created as mentioned above. It is made as [input / into the IC chip 11 / a magic number (magic number), the enciphered magic number (encrypted magic number), and the enciphered information (cipher text)]. What was reproduced from DVD1 is supplied as an enciphered magic number, from the memory, reading appearance of what was held as a magic number in the memory which the DVD player itself does not illustrate is carried out, and it is supplied. This magic number is the train of a predetermined figure or an alphabetic character decided beforehand, and is the same as that of the magic number which is an encryption side and was used.

[0042] Memory 12 is made as [hold / the cryptographic key K0 shown in drawing 1 , i.e., a master key,]. As a register 13 is mentioned later, it is made as [hold /, cryptographic key (work key), i.e., work-piece key, of the predetermined generation searched for using the above-mentioned function F from the master key,]. Based on the master key by which reading appearance was first carried out from the inputted magic number, the enciphered magic number, and memory 12, the decryption circuit 14 creates a work-piece key, and is made as [supply / to a register 13 / the created work-piece key] so that it may mention later. And the decryption circuit 14 decrypts the inputted information (Cipher Text) which was enciphered using a work-piece key, and is made as [output / as plaintext data (Plain text)].

[0043] Next, the flow chart shown in drawing 6 is referred to, and the procedure which decrypts the enciphered information which was recorded on DVD1 in the IC chip 11 is explained. First, in step S11, reading appearance of the enciphered magic number which was recorded on the predetermined location of DVD1 is carried out. Next, it progresses to step S12, and from the enciphered magic

number by which reading appearance was carried out in step S11, and the magic number by which reading appearance was carried out from the memory which the DVD player itself has, and which is not illustrated, as it mentions later with reference to the flow chart of drawing 7 , it asks for a work-piece key.

[0044] Drawing 7 is a flow chart for explaining the detail of the processing in step S12 of drawing 6 . First, in step S21, reading appearance of the master key is carried out from the memory 12 of the IC chip 11, and let this be a selection key (k). And this selection key (k) is supplied to the decryption circuit 14. Here, a selection key (k) shall express the cryptographic key by which current selection is made.

[0045] Next, it progresses to step S22 and the decryption circuit 14 decrypts the supplied magic number (MNe) which is enciphered using a selection key (k). And it judges whether the result of having decrypted the magic number enciphered by the selection key (k), and a magic number are in agreement. When judged with the magic number which is not enciphered as the decrypted result not being in agreement, it is judged with this selection key not being a cryptographic key which enciphered the magic number enciphered at the encryption side. Therefore, as it progresses to step S23 and is shown in a degree type (5), the next generation's cryptographic key is calculated using a one-way function (F) from a selection key (k), and newly let it be a selection key (k).

[0046] k=F (k) ... (5)

[0047] And return and the same processing as the case where it mentions above are again repeated and performed to step S22.

[0048] The result of on the other hand having decrypted the magic number enciphered by the selection key (k) in step S22, and when it is judged with the magic number which is not enciphered being in agreement, a selection key (k) is set to an encryption side. it is judged with it being the cryptographic key which enciphered the enciphered magic number -- therefore, it progresses to step S24, and the decryption circuit 14 uses this selection key (k) as a work-piece key, supplies it to a register 13, and is stored in a register 13. And processing of the

flow chart of this drawing 7 is ended, and it returns to processing of the flow chart of drawing 6 .

[0049] Then, it progresses to step S13 of the flow chart of drawing 6 , and the decryption circuit 14 reads the work-piece key called for in step S12 (step S21 of drawing 7 thru/or 24) from a register 13, it decrypts the inputted information (Cipher Text) which is enciphered using a work-piece key, and outputs it as plaintext data (Plain Text).

[0050] Thus, since the IC chip 11 asks for WAKUKI corresponding to the enciphered information and decrypts the inputted information which was enciphered from a master key using this work-piece key, it only holds the master key and can decrypt the information enciphered by the cryptographic key of the hierarchy of arbitration.

[0051] When the software of a computer performs processing which was mentioned above, processing of step S12 of drawing 6 came to be shown in drawing 8 . That is, drawing 8 is a flow chart which shows the procedure in which the enciphered information is decrypted in the computer which realizes a function as shown in drawing 5 by software. In this case, the computer contains a decode substrate which corresponds to drawing 5 , and software is memorized by the memory of that substrate. Moreover, the master key beforehand memorized by memory in this case is not used, but the newest cryptographic key (there may be a master key) distributed is used.

[0052] for example, a predetermined hierarchy's cryptographic key (Ki) which was printed by DVD and distributed to it so that it might mention later with reference to drawing 9 -- (-- here -- i -- n and n- 1, ..., or 1 --) -- a user inputs into a computer through a keyboard. The cryptographic key is made as [memorize / the predetermined memory in a computer]. Or a computer receives the newest cryptographic key distributed through the telephone line or a network, and is made as [memorize / in predetermined memory (for example, RAM) / it].

[0053] First, in step S31, reading appearance of a predetermined hierarchy's inputted cryptographic key (Ki) is carried out from memory, and let it be a

selection key (k). Here, a selection key (k) shall express the cryptographic key by which current selection is made like the case where it mentions above.

[0054] Next, the magic number progressed and enciphered is decrypted by step S32 using a selection key (k). And it is judged whether the result of having decrypted the magic number enciphered by the selection key (k), and a magic number are in agreement. When judged with the magic number which is not enciphered as the decrypted result not being in agreement, it is judged with a selection key (k) not being a cryptographic key which enciphered the magic number to the encryption side. Therefore, as it progresses to step S33 and was shown in the above-mentioned formula (5), the next generation's cryptographic key is calculated using a one-way function (F) from a selection key (k), and newly let it be a selection key (k).

[0055] And return and the same processing as the case where it mentions above are again repeated and performed to step S32.

[0056] When judged with the result and magic number which decrypted the magic number enciphered by the selection key (k) in step S32 on the other hand being in agreement, it is judged with a selection key (k) being a cryptographic key which enciphered the magic number to the encryption side. Therefore, it progresses to step S34, this selection key (k) is used as a work-piece key, and this work-piece key is memorized by predetermined memory (for example, register). And processing of the flow chart of this drawing 8 is ended, and it returns to processing of the flow chart of drawing 6 .

[0057] After that, it progresses to step S13 of the flow chart of drawing 6 , the enciphered information is decrypted using the work-piece key called for in step S12 (step S31 of drawing 8 thru/or S34), and it outputs as plaintext data (Plain Text).

[0058] Thus, based on the cryptographic key of the hierarchy of the arbitration distributed when information enciphered was decrypted by the software of a computer, the information enciphered by the cryptographic key (Ki) or the cryptographic key (Ki-1 thru/or K1) of a hierarchy lower than the hierarchy of the

cryptographic key at least can be decrypted.

[0059] Thus, it sets in the gestalt of operation of this invention. Since the information enciphered by the cryptographic key before it can also be decrypted based on the newest cryptographic key (it is possible also in a master key and possible also in the cryptographic key of the hierarchy of arbitration) Whenever a cryptographic key is decoded and a cryptographic key is changed like before that what is necessary is to memorize only the newest cryptographic key, in addition to the cryptographic key before it, memorize a new cryptographic key, and it becomes unnecessary to manage, and management of a cryptographic key can be made easy.

[0060] Moreover, in the gestalt of operation of drawing 5 , since the memory 12 of a chip 11 is made to memorize a cryptographic key (master key), the cryptographic key of a hierarchy predetermined within the chip is calculated and the enciphered information was decrypted, it can control that a cryptographic key leaks outside and decode of a cryptographic key can be made difficult. Furthermore, in the gestalt of the above-mentioned implementation, since it was made to perform calculation processing of a work-piece key, and decryption processing of the enciphered information in the same decryption circuit 14, a configuration can be simplified.

[0061] Next, how to distribute a cryptographic key is explained with reference to drawing 9 thru/or drawing 11 .

[0062] Drawing 9 shows the example which prints and distributes a cryptographic key to the case and the DVD itself of DVD.

[0063] For example, the alpha character corresponding to a predetermined hierarchy's cryptographic key A, a figure, a bar code, or a hologram is printed on the case of DVD21 where Title A was recorded, the front face of DVD21 the very thing, etc. Similarly, the alpha character corresponding to a predetermined hierarchy's cryptographic key B, a figure, a bar code, or a hologram is printed on the case of DVD22 where Title B was recorded, the front face of DVD22 the very thing, etc. Thus, cryptographic key B can be distributed [DVD /21] for

cryptographic key A to a user with DVD22 again.

[0064] Or it is also possible to record the data which express cryptographic key A with record media, such as an IC card, to record the data which express cryptographic key B with record media, such as an IC card, again with DVD21, and to make it distribute with DVD22.

[0065] When reproducing DVD21, a user uses the input units 24, such as a keyboard, for a computer 23, and inputs into it cryptographic key A printed by DVD21. With reference to the flow chart of drawing 8 , the computer 23 is made as [perform / with a predetermined application program / the function which decrypts the information which the IC chip 11 shown in drawing 5 performs, and which was functioned namely, enciphered], as mentioned above.

[0066] next, if it sets in the DVD reader which does not illustrate DVD21, a computer 23 will carry out reading appearance of the information enciphered from DVD21 through a DVD reader, and will decrypt the information which carried out reading appearance from DVD21 and which is enciphered based on cryptographic key A inputted previously. The information which was recorded there about DVD22 as well as the case of DVD21 and which is enciphered can be decrypted.

[0067] Therefore, this example is suitable when distributing a different cryptographic key for every title of DVD (for example, when assigning the cryptographic key calculated by the one-way function from a different master key for every title of DVD).

[0068] For example, even when cryptographic key A corresponding to Title A is decoded, cryptographic key A corresponding to Title A is updated by the cryptographic key A2 of the hierarchy on it and the sequel of Title A is enciphered by the cryptographic key A2, as mentioned above with reference to drawing 8 , it can ask for cryptographic key A before being updated easily by the predetermined operation from a cryptographic key A2. Therefore, a user can decrypt the title A enciphered by the former cryptographic key only using the newest cryptographic key (cryptographic key A2 in this case).

[0069] Drawing 10 shows the example which inserts and distributes the code which expresses a cryptographic key with the software for decrypting a cryptographic key.

[0070] That is, the code showing a cryptographic key is inserted into the software for the decryption prepared in the decryption substrate 33 which decrypts encryption information. And a computer 23 is equipped with this decryption substrate 33. Thereby, a computer 23 can decrypt the enciphered information which was recorded on DVDs 31 and 32 through the decryption substrate 33, and can output the animation corresponding to the decrypted information, a still picture, voice, etc.

[0071] This example does not depend on the title of DVD, but when distributing the same cryptographic key, it is suitable.

[0072] Moreover, in the case of this example, it is also possible to connect a computer 23 to the telephone line or a network, and to distribute the updated cryptographic key to a computer 23 through the telephone line or a network. A computer 23 is made to memorize in the software for a decryption of the newest cryptographic key distributed through the telephone line or a network of the decryption substrate 33.

[0073] And using this cryptographic key, as the computer 23 was mentioned above with reference to drawing 6 and drawing 8 , it can decrypt the information recorded on DVDs 31 and 32.

[0074] Moreover, the information enciphered by the cryptographic key through the telephone line or a network is transmitted, and it can provide for a computer 23. In this case, a computer 23 decrypts this information using the cryptographic key previously distributed through the telephone line or a network.

[0075] By the way, as mentioned above with reference to drawing 1 , from the first hierarchized cryptographic key (K0), all hierarchies' cryptographic key can be formed using a one-way function (F), and this cryptographic key K0 can be used as a master key. Then, all hierarchies' cryptographic key can be created from this cryptographic key K0, and it can make it possible to decrypt also for the

information enciphered by which cryptographic key (K1 thru/or Kn) by embedding the cryptographic key K0 used as this master key into hardware, such as an integrated circuit. For a regular user, since it is difficult to decode the data embedded to hardware, such as an integrated circuit, it can do in this way and the unauthorized use of a cryptographic key can be controlled.

[0076] Drawing 11 shows the example which embeds and distributes a cryptographic key to the integrated circuit in this way. In this drawing, the integrated circuit 41 which memorizes a master key is manufactured by the manufacturer who has a predetermined secrecy obligation. The IC chip 11 shown in drawing 5 is applicable to this integrated circuit 41. And after in the case of this example this integrated circuit 41 is supplied to Manufacturer A and built into the DVD player 43 by Manufacturer A, it is provided for a user.

[0077] On the other hand, the magic number enciphered using a predetermined hierarchy's cryptographic key which an integrated circuit 41 memorizes, and the predetermined encryption information enciphered using this cryptographic key are recorded on DVD42.

[0078] If a user sets DVD42 to the DVD player 43, as reading appearance of the master key is carried out from an integrated circuit 41 and it mentioned above with reference to the flow chart of drawing 6 and drawing 7 , a work-piece key will be called for, the enciphered information which was recorded on DVD42 will be decrypted, and a corresponding animation, a still picture, and voice will be outputted.

[0079] Thus, when a master key is stored in an integrated circuit 41, the DVD player 43 can make the enciphered information which was recorded on DVD42 decrypt and output, though the information recorded on DVD42 was enciphered by which hierarchy's cryptographic key.

[0080] Moreover, the cryptographic key of the predetermined hierarchy of the cryptographic keys which use and calculate a one-way function not from a master key but from a master key is stored in an integrated circuit 41, and things are also made to it. In that case, when the information enciphered by the

cryptographic key or the cryptographic key of a hierarchy lower than the cryptographic key is recorded on DVD42, the DVD player 43 can decrypt the information recorded on DVD42.

[0081] Thus, the approach of storing a predetermined cryptographic key in a predetermined integrated circuit, and including it in the DVD player 43 is suitable, when not depending on the title of DVD but distributing the same cryptographic key.

[0082] As mentioned above, a cryptographic key is hierarchized using a one-way function, and while enciphering information among the hierarchized cryptographic keys using the cryptographic key of the hierarchy of arbitration, by distributing this cryptographic key to a user, a user only holds the newest cryptographic key and can also decrypt the information enciphered by the former cryptographic key. Thereby, a cryptographic key is easily manageable.

[0083] For example, the gestalt of operation shown in drawing 11 can be applied more to validity, when a cryptographic key cannot be especially exchanged easily through a network etc. That is, since the integrated circuit 41 has memorized the master key when the information on software, an animation, etc. is enciphered and recorded on DVD42 by a predetermined hierarchy's cryptographic key, the cryptographic key of the hierarchy of arbitration can be created using a one-way function (F) from this master key, and the information enciphered by a predetermined hierarchy's cryptographic key currently recorded on DVD42 can be decrypted.

[0084] Thereby, a cryptographic key is decoded and updated, without being conscious especially as usual, it can be decrypted and a user can be reincarnated, even if the information enciphered by DVD42 by a new hierarchy's cryptographic key is recorded.

[0085] Moreover, in the DVD player which does not have the integrated circuit 41 which memorizes a cryptographic key, since DVD42 with which the information enciphered by this cryptographic key was recorded is correctly unreproducible, informational utilization can be restricted appropriately. In the computer which

similarly does not have the decode substrate which memorizes a cryptographic key, since the record medium with which the information enciphered by this cryptographic key was recorded is correctly unreproducible, informational utilization can be restricted appropriately.

[0086] Furthermore, the alpha character with which a cryptographic key is expressed to record media, such as DVD, or the case of those, Store the data corresponding to a cryptographic key in an IC card, or [printing a figure, a bar code, or a hologram] An unauthorized use makes the data corresponding to a cryptographic key (for example, master key) memorize in a difficult integrated circuit, or Into the software for a decryption, the data corresponding to a cryptographic key can be inserted, or it can transmit through the telephone line or a network, and a cryptographic key can be distributed very easily.

[0087] In addition, in the gestalt of the above-mentioned implementation, although DVD was used as a record medium, it is also possible for it not to be limited to this, of course and to use the record medium of others, such as CD-ROM, MD (mini disc) (trademark), an optical disk, a magneto-optic disk, or a floppy disk.

[0088] Moreover, through networks, such as the Internet, this invention can be applied, also when offering information.

[0089] Furthermore, in the gestalt of the above-mentioned implementation, although the DVD player itself held the magic number in predetermined memory etc., it is possible to record on the predetermined location of DVD, to read it for example, and to make it also make it input into the decryption circuit 14. In that case, as shown in drawing 4 , a magic number is supplied to a recording apparatus 54, and is recorded on a disk 1. Moreover, although made as [decrypt / with software / the information enciphered], IC chip is built in a computer and you may make it make decode actuation perform for IC chip in a computer, without using software. In this case, since the computer which does not have the integrated circuit 41 which memorizes a cryptographic key cannot decrypt the enciphered information correctly, it can restrict informational utilization

appropriately.

[0090] In addition, various deformation and applications can think in the range which does not deviate from the main point of this invention. Therefore, the summary of this invention is not limited to the gestalt of operation.

[0091]

[Effect of the Invention] Since the cryptographic key was hierarchized like the above using the one-way function according to the encryption approach according to claim 1, the record approach according to claim 4, encryption equipment according to claim 15, and the record medium according to claim 26 In a decryption side, the information enciphered by the old cryptographic key can also be decrypted only by holding the newest cryptographic key, and it becomes possible to make easy the generation control of a cryptographic key when a cryptographic key is updated.

[0092] Moreover, since it was made to decrypt using the cryptographic key hierarchized using the one-way function according to the decryption approach according to claim 6 and decryption equipment according to claim 18, the information enciphered by the old cryptographic key can also be decrypted only by holding the newest cryptographic key.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the example of the layered structure of the cryptographic key applied to the encryption approach of this invention.

[Drawing 2] It is the flow chart which shows the procedure which creates DVD which recorded the enciphered information.

[Drawing 3] It is drawing showing DVD with which the information enciphered as the enciphered magic key was recorded.

[Drawing 4] It is the block diagram showing the example of a configuration of the encryption equipment in this invention.

[Drawing 5] It is the block diagram showing the example of a configuration of the chip 11 which decrypts the information recorded on DVD of drawing 3 .

[Drawing 6] It is a flow chart for explaining actuation of the chip 11 of drawing 5 .

[Drawing 7] It is a flow chart for explaining the detail of step S12 of drawing 6 .

[Drawing 8] They are other flow charts for explaining the detail of step S12 of drawing 6 .

[Drawing 9] It is drawing for explaining how to print and distribute a cryptographic key to DVD.

[Drawing 10] It is drawing for explaining how to insert a cryptographic key in the software for a decryption, and to distribute it.

[Drawing 11] It is drawing for explaining how to embed and distribute a cryptographic key to an integrated circuit.

[Drawing 12] It is drawing showing the principle of encryption and a decryption.

[Description of Notations]

1 Disk 11 Chip 12 Memory 13 Register 14 Decryption Circuits 21 22 DVD 23 Computer 31, 32DVD 33 Decryption Substrate 41 Integrated Circuit 42 DVD 43 DVD Player